Information Interfaces for Process Plant Diagnosis

Lind, Morten

Publication date:
1984

Document Version
Publisher's PDF, also known as Version of record

Risø-M-2417

RISØ

Risø-M-2417

Information Interfaces for Process Plant Diagnosis

Morten Lind

Risø National Laboratory, DK-4000 Roskilde, Denmark
February 1984

RISØ-M-2417

INFORMATION INTERFACES FOR PROCESS PLANT DIAGNOSIS

Morten Lind

Abstract: The paper describes a systematic approach to the design of information interfaces for operator support in diagnosing complex systems faults. The need of interpreting primary measured plant variables within the framework of different system representations organized into an abstraction hierarchy is identified from an analysis of the problem of diagnosing complex systems. A formalized approach to the modelling of production systems, called Multilevel Flow Modelling, is described. A MFM model specifies plant control requirements and the associated need for plant information and provide a consistent context for the interpretation of real time plant signals in diagnosis of malfunctions. The use of MFM models as a basis for functional design of the plant instrumentation system is outlined, and the use of Knowledge Based (Expert) Systems for the design of man-machine interfaces is mentioned. Such systems would allow an active user participation in diagnosis and thus provide the basis for cooperative problem solving.

INIS Descriptors CONTROL SYSTEMS; DIAGNOSIS; FLOW MODELS; HUMAN FACTORS; INDUSTRIAL PLANTS; INFORMATION; INTERFACES; MAN-MACHINE SYSTEMS; NUCLEAR POWER PLANTS

UDC 007.51 : 62-5 : 65.015.11

February 1984
Risø National Laboratory, DK 4000 Roskilde, Denmark

Presented at the conference on Data Communication in Distributed Systems, organised by the Danish Automation Society, November 2-3, 1983.

ISBN 87-550-0982-4
ISSN 0418-6435

Risø Repro 1984

CONTENTS

INTRODUCTION

The importance of the human operator as a systems supervisor and problem solver in diagnosis of plant malfunctions is widely recognized. But the operator seems at the same time to be a potential source of error in today's complex systems, and most attempts to improve total systems reliability usually involve the increase of the level of automation. The resulting reduction of the operators' direct involvement in plant control leads to the deterioration of his working conditions . However, in many cases the problem is not that the operator is potentially unreliable, but that the man-machine interface is not designed to support the operator with the information needed for making appropriate decisions. From that perspective you would not expect that the operator could respond properly.

The development of distributed microprocessor-based control and instrumentation systems give some hope for the improvement of this situation. But a change in the design of the overall systems control strategy will be required. There are two reasons for this need. First, the application of the new information technology will lead to an increase in total system complexity, and a systematic design approach is necessary. This will both ensure that the information processing capability which is available is properly used and will also ensure the achievement of a properly functioning system. Second, it is important tc ensure that the operating staff is properly integrated into the decision making complex involved in plant control.

Such a systematic approach has been proposed in (Rasmussen & Lind, 1982) and in (Rasmussen, 1983). The basic idea is to adopt a top-down strategy in the design by identifying plant control requirements and define the decision making functions necessary to perform the required control tasks. Control requirements are specified independently of the actual implementation of the control functions and the control systems designer, the operator and the control computer are considered

as cooperating decision makers (for details see Rasmussen, 1983). Two other aspects are involved in the design approach, a description of the contexts wherein decisions are made and a description of the strategies used for making decisions.

In the following we will only deal with one of these aspects. We will discuss the context wherein decisions should be made in diagnosis of plant disturbances. This will comprise a discussion of the problem of identifying the state of complex systems and of the plant information required for this task. This will involve the embedding of processed real time sensor signals within the context of plant design information. In this way a proper context is provided for the interpretation of plant signals. The strategies used for diagnosis will not be dealt with here as they are described elsewhere (Rasmussen, 1981). Furthermore, we will not describe how graphics displays or other types of interface technology can be used for communicating this decision context to the operating staff. This aspect has been covered by Goodstein (1982). We will here be concerned only with the definition of the information interface required. The design of the instrumentation system necessary to support such an interface will also be discussed, and the use of Expert Systems for the implementation of user-friendly diagnostic aids will be mentioned.

THE STATE IDENTIFICATION PROBLEM IN COMPLEX SYSTEMS

The identification of the state of a process plant is necessary as a basis for the planning of compensating control actions. However, due to the complexity of a process plant, it is not possible to define a single state concept as known in linear systems theory or automata theory which is adequate for the range of control tasks encountered in plant operation. The problem is that the very high number of degrees of freedom potentially available in the plant creates a wide variety of

possible modes of interaction between subsystems or components. These interactions are closely controlled during planned start--up, shut-down and normal production situations. But in the case of plant disturbances such as component failure or sudden unexpected changes in production requirements (e.g. loss of turbine-generator load in power plants) will the detailed nature of these interactions depend on the actual disturbance. A disturbance may initiate automatic protective systems leading to a change in the functional structure of the plant. Other disturbances may only lead to perturbations of plant variables and thus leave the plant functionally intact. In the case of frequent familiar disturbances the operator can readily recognize the state of the plant and the associated control task, and the control actions to be made can either be remembered or found in documented operating instructions. But, in the event of unfamiliar disturbances, the operator is faced with a difficult decision problem his main problem (if he at all realize he has a problem and does not stick to stereotyped responses) is to identify the nature of the control problem, i.e. whether the situation requires protective action because plant safety is threatened or the situation only require corrections to maintain production in spite of the disturbance or a faulted component should be located and repaired.

The operator's main problem is to prioritize between safety and production. If safety is endangered then only the state of a relatively small set of critical variables should be known in order to make a control decision or to verify that automatic protective actions has occurred as required. In more fuzzy situations, the operator may try to keep the plant running to prevent production losses even if safety is endangered. When the operator judges that a protective action is required he may have several possibilities - he may prefer to win time for decisions or he may wish to be able to make a quick start-up. In order to do this, the operator requires more detailed information in order to be able to evaluate whether sufficient degrees of functional freedom are available for compromising between safety and availability goals, i.e. to identify the means to be used to reach the desired ends. A factor which adds

to the complexity of the state identification problem is the need for making decisions within a time interval which cannot be determined before the actual plant state has been identified. This means that during emergency situations the operator has in general to deal with a problem which is not well structured. The level of information required for identifying the plant state depends on the goal to pursue and the choice of goal depends on the plant situation. In order to deal with this circularity, the operator must search through the available information and use heuristics to control the task. In fact this is what is required of the operator in control rooms equipped with conventional alarm and indicator panels providing plant information on essentially the raw sensor level. It is expected that the operator is able to provide a proper interpretation of complex patterns of alarms and instrument indications on the basis of his general process knowledge acquired by training and operational experience. This is clearly an impossible task in the case of unfamiliar disturbances.

Recent developments of information systems, based on display concepts using mimic diagrams of the plant as a framework for information presentation do not provide a satisfactory solution to the problems stated above. This is because higher level control requirements dealing with the state of plant functions cannot be specified on the level of systems, equipment or components. An approach to design of information interfaces which support decision making in tasks ranging from the control of the operation of a plant component to control of the overall production state has been proposed in (Rasmussen & Lind, 1981). The main idea is to use a computer-based man-machine interface which processes the measured plant information and communicates it to the operator within the framework of a hierarchy of plant descriptions on different levels of abstraction. The abstraction hierarchy and an associated formalized functional decomposition hierarchy based on a system modelling technique called Multilevel Flow Modelling (or MFM for short) will be discussed below. The abstraction hierarchy relate directly to plant information generated during process design and describe

different contexts for the operators decision making. The MFM models serve to identify plant control requirements on all levels of plant function independently of the actual implementation of control functions, i.e. do not distinguish between automated or manual controls. It furthermore serves to identify the information required to make control decisions and provide the basis for a systematic design of the control and instrumentation systems. The problem of control design will not be discussed here as it has been considered in detail elsewhere (Lind, 1979 and 1983). Here we will consider the design of computer based instrumentation systems which can support an advanced information interface appropriate for diagnostic support of operators as proposed in op.cit.

THE ABSTRACTION HIERARCHY

The properties of process plants can be described by using an abstraction hierarchy as shown in Figure 1 (Rasmussen, 1979). This hierarchy provides a multiple view of the same system in that each level emphasizes certain selected aspects of system function. Abstraction hierarchies are used as overall modelling frameworks within several problem areas related to the topic considered here. As examples could be mentioned Computer Aided Design (Eastman, 1978), System Theory (Mesarovic et al., 1970) and Artificial Intelligence (Sussman et al., 1980).

On the highest level of abstraction, the level of functional purpose, the system is described by its purpose, i.e. in terms related to its interaction with the environment. On this level, a power plant would thus be described as an energy production system since this description is adequate for dealing with its interaction with the environment, which consists of the electric distribution network and the consumers. When we shift a level down to the level of abstract function, we describe the internal function of the system in terms of the topology of the

flow of energy, mass and information. This type of description represents the overall processes performed by the system considered and ignores physical details on how these processes are implemented. These details are described on the next lower levels. Returning to the abstraction hierarchy on Figure 1, the system can also be described on the level of generalized function in terms of the behaviour of functionally integrated subsystems. In power plants, we can talk about the air-gas path in the boiler and the component cooling system etc. and the behaviour in terms of states of and interaction between these systems. In the example of a watch given by Sussman et al. (1980) this level provides a description in terms of balances, escapement and wheel-trains etc. Moving down to the level of physical function, the system is described in terms of interactions between components and equipment; i.e. valves, pumps, turbine generator units etc. This is the level which is usually described in a piping and instrumentation diagram. On the lowest level of abstraction we deal with the physical anatomy, material form and location in space.

As depicted in Figure 1, the abstraction hierarchy organizes the different levels according to the degree with which they represent system properties related to the overall plant purpose or to the implementation in terms of physical components. At each level of abstraction, the reasons and specifications, i.e. the requirements for proper function, are formulated from above, and the means for control and potential for function, i.e. the physical capabilities and limitations are coming up from below. In case of disturbances due to technical faults, the causes of malfunction are propagating bottom-up through the hierarchy of abstraction, at the same time as rules for proper functions and target states are derived top-down.

The abstraction hierarchy is a useful basis for discussing a formalized process design. But at the same time it is useful for the state identification problem as discussed previously. A given disturbance can be described on any level in the abstraction hierarchy provided the measured plant information

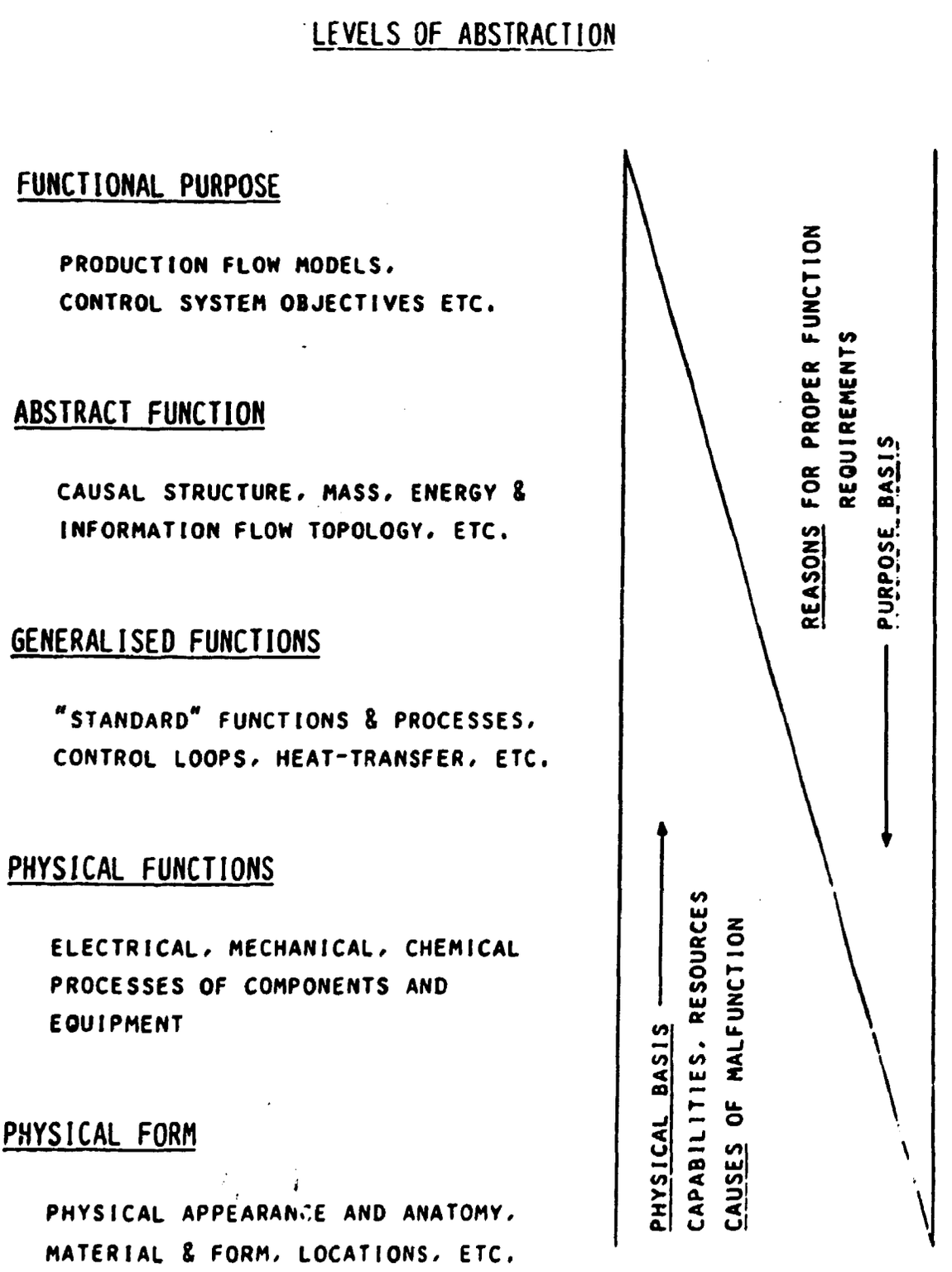


Figure 1. Abstraction hierarchy used for representing the functional properties of a technical system.

can be related to state information relevant to the individual levels. This will be discussed later in the section on data integration. From the point of view of operator support in state identification, this hierarchy is important because it defines different ways of describing the same phenomena and constitutes a framework for integrating plant information of the same system within different contexts. Thus a description of the system on the level of physical function may enable the operator to take advantage of component-specific knowledge as e.g. pump characteristics in diagnosis; this is not possible on the higher levels which deal with more abstract and general concepts. On these levels, the universal laws of mass and energy conservation can be applied for making inferences using e.g. a search in the causal mass and energy flow topology. On this level inferences can be made independent of the nature of the given disturbance, but the plant state is identified with low resolution and it may be ambiguous. On the other hand on the level of physical function it is possible to characterize a disturbance in terms of component or equipment failure. On this level, a search in the physical topography may be applied combined with a search in a library of symptoms. The strategy chosen depends on the actual situation and may involve shifts in level of abstraction. Accordingly, the abstraction hierarchy can be considered as a structure for controlling the use of different types of plant information during plant state identification.

CHARACTERISTICS OF SYSTEM COMPLEXITY

The notion of an abstraction hierarchy emphasize the need of different levels of descriptions when modelling a technical system. The complexity of designing and operating large processing units is partly due to the need of applying multiple perspectives on the system. But another factor which is important is the nature of relations between "objects" on

different levels.

In order to identify these relations we will consider the overall production and safety goals of e.g. a nuclear power plant which are to maintain electricity production and to prevent the release of radioactive materials to the environment. Each of these goals can be approached by proper control of various functions related to inventory and heat balances in the plant system, and each function can in general be implemented by means of different equipment and configurations. Furthermore, each piece of equipment may support several plant functions. These many to many mappings (Figure 2) among the levels in the abstraction hierarchy contribute to system complexity. Control problems occur if several conflicting goals should be achieved by means of the same plant functions. But at the same time provide the many to many mappings also the potential for corrective actions by operators or automated controls, since they make it possible to replace a disturbed function by the service of other equipment. This reflect the use of redundancy or diversity techniques in the design for reliable and safe system operation.

Another factor contributing to complexity has to do with the conditions to be satisfied during plant operations in order to ensure proper system integrity and function. The nature of these conditions can be realized by considering the start-up or shut-down of complex systems. An example representing a subsequence from the start-up of a conventional fossil fired drum boiler is shown for illustration in Figure 3. The figure shows how a particular part of the start-up is accomplished by a sequence of control actions. By a closer examination of these sequences three control tasks can be identified, one dealing with changes of system configuration, one dealing with the control of a mass balance and one dealing with the control of an energy balance. The configuration control task serves to make available the necessary system equipment and physical interconnections required to establish part of the function provided by the feedwater system. The mass balance control serves to provide the condition necessary to support the

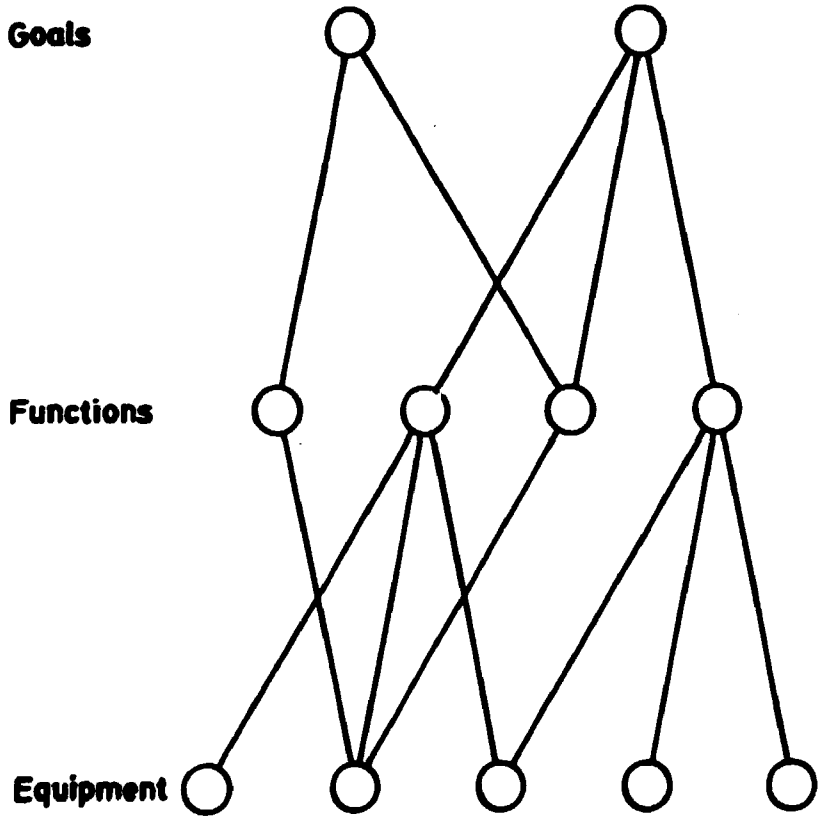


Figure 2. Systems complexity is due to many-to-many mappings between goals, functions and equipment.

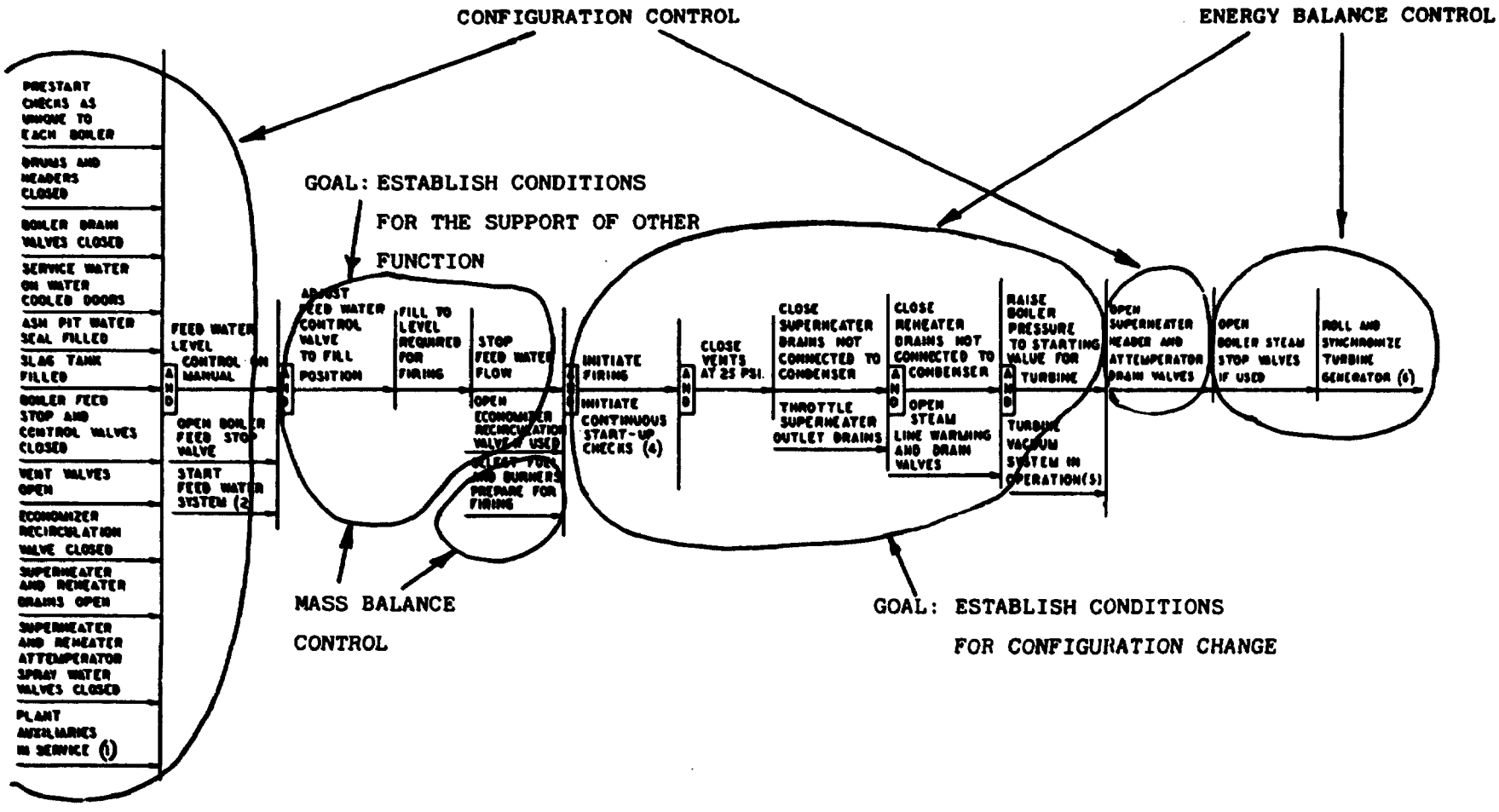


Figure 3. Section of a start-up sequence for a fossil fired steam boiler, (sequence taken from West, 1973).

functions required in the energy balance control (the drum should be filled with water before heating can start). The energy balance control serves to provide the conditions required for starting up the turbine and is a preparation for the syncronization of the turbine to the grid.

In terms of the abstract notions of goals, functions and equipment introduced in Figure 2 there are accordingly three types of conditions, one relates to the conditions necessary to ensure that a certain plant function exists (this will be called a support condition), another type deals with conditions necessary to ensure that the equipment (including its configuration), necessary for a certain plant function, is available (an availability condition). The third type of condition deals with the situation where system reconfiguration is conditioned by the proper state of a plant function (a switching condition).

As these conditions should be satisfied in an orderly way in order to establish system functions complex systems are usually operated in a well-defined set of operating modes. Each mode is characterized by a unique functional structure as illustrated in Figure 4. It is an important part of the design of information interfaces to identify these modes and to specify control requirements related to each individual mode. Information requirements and the instrumentation system necessary to support the information interface will also in general change with the operating mode.

MULTILEVEL FLOW MODELLING FOR FUNCTIONAL SPECIFICATION

A consistent description of plant properties in a purpose - function - equipment hierarchy is accordingly an important basis for the design of overall plant control strategies involving the identification of control tasks and the subse-

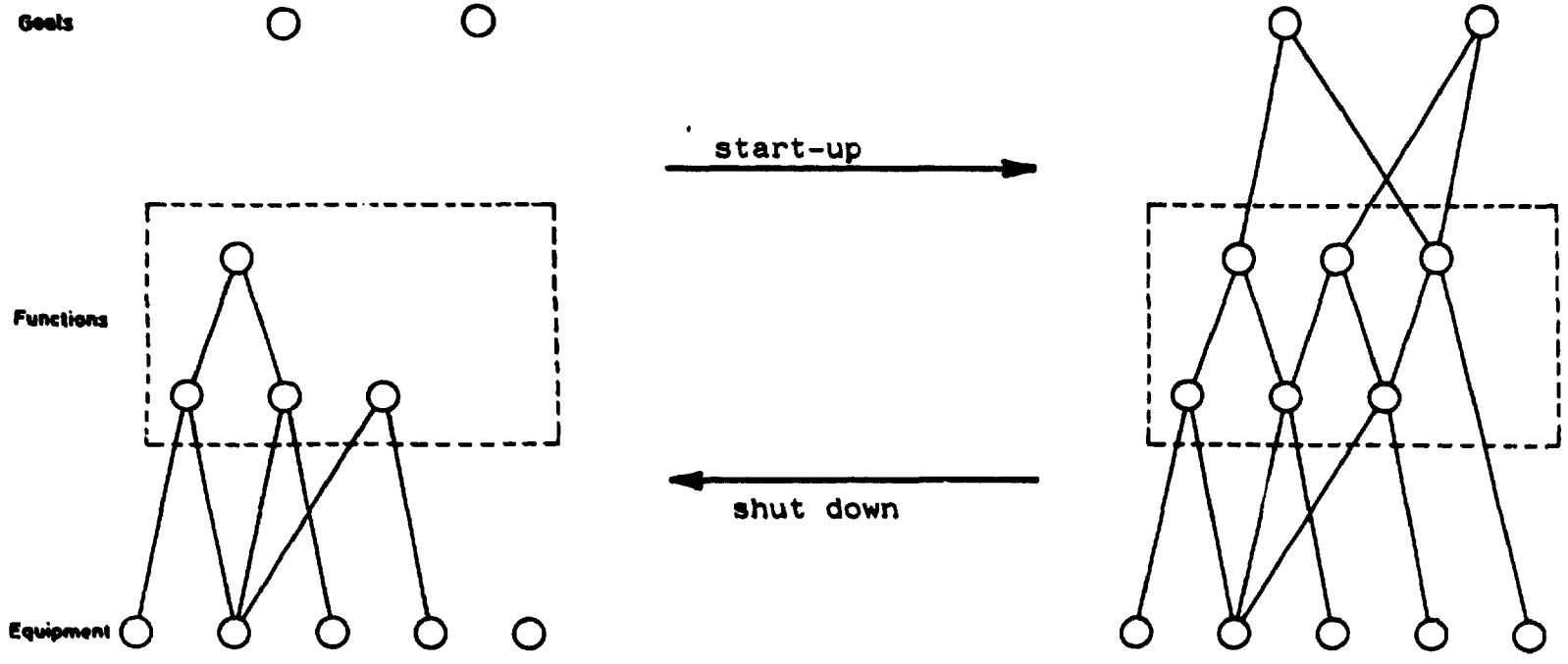


Figure 4. The functional structure of complex systems change during start-up and shut down.

quent allocation of tasks between operators and automated control and protection systems. Such a system description would also provide a basis for design of operator support systems for diagnostic and supervisory purposes (Rasmussen and Lind, 1981). An approach to such a plant description has been made by Westinghouse (Rumancik et al., 1981) for the specification of a disturbance and surveillance system (DASS). Figure 5 shows an example from op.cit. of a nuclear power plant description identifying critical safety requirements and functions. The levels in this description define goals, functions and equipment involved in safe operation of a PWR power plant. However, this type of description is not based on a formalized modelling framework and the approach may include inconsistencies or ambiguities. The multilevel flow modelling method (MFM) developed by the present author provides a formalism for consistent specification of plant functions and control requirements. A detailed description of the MFM method is given in (Lind, 1983), here we will only give a summany of the basic features of the method.

In multilevel flow modelling the functional structure of process plants is described in terms of a set of interrelated mass and energy flow structures related to different levels of physical aggregation. The basic concepts used are closely related to thermodynamics which is the basis for every consistent approach to modelling physical phenomena in process plants. The methodology is used to provide normative models, as the aim is to describe plant goals and functions as specified in the process design. The flow modelling concepts may also be used for descriptive purposes. A descriptive model represents the actual behaviour of the system, whereas a normative model represents the system in terms of how it is intended to behave (Simon, 1981). The modelling approaches in the two cases are basically different as the normative model requires a top-down function-oriented holistic approach whereas the descriptive modelling is a bottom-up atomistic approach starting with minute details and ending with a level of detail determined by simplifying assumptions. The MFM method distinguish between two groups of modelling concepts, one related to the representation

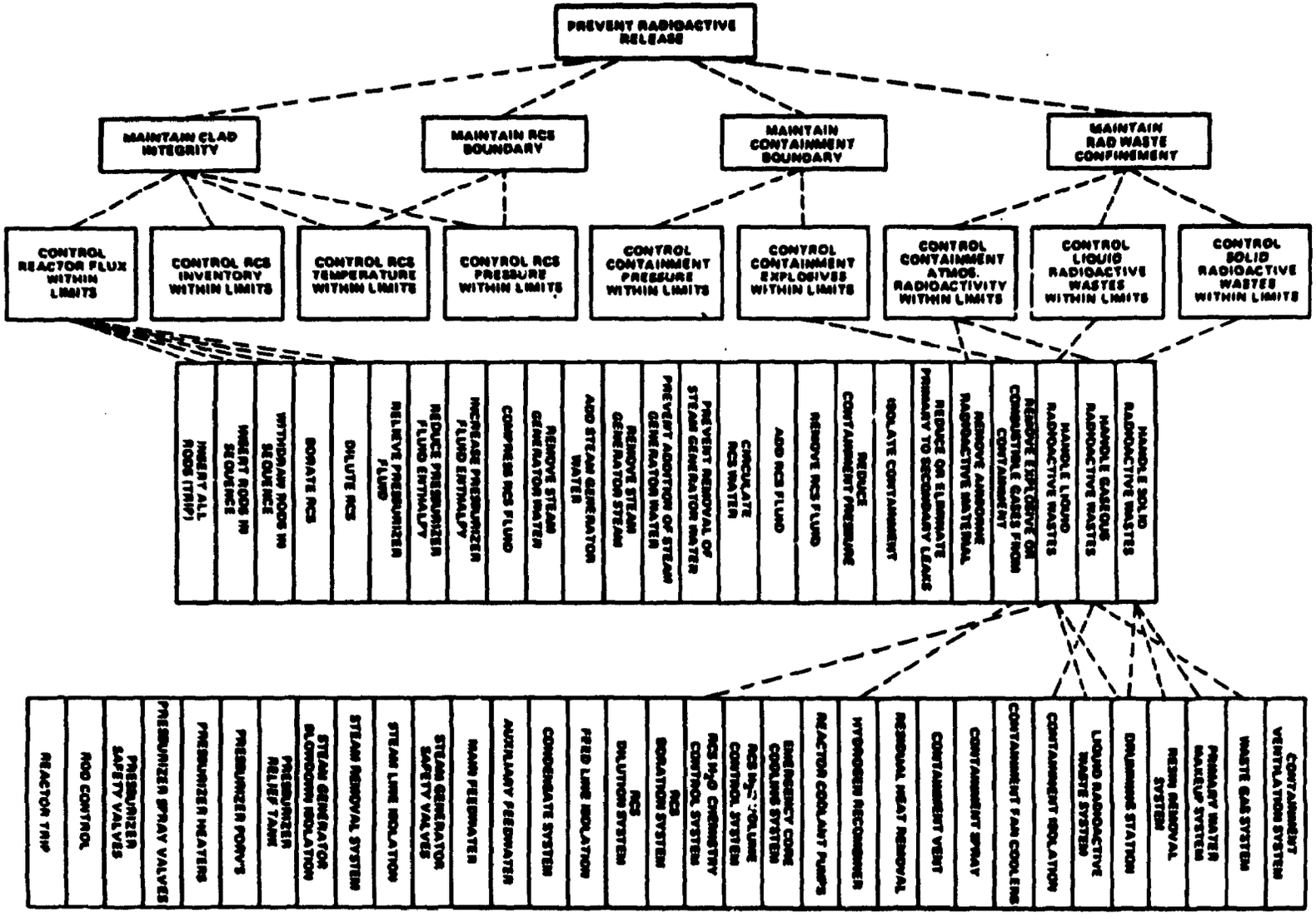


Figure 5. Critical safety requirements and functions chart. (From Rumancik et. al., 1981).

of plant goals and functions, the socalled flow functions, the other group deals with the representation of how flow functions are realized. Here we will only deal with the representation of system functions and refer the reader to (Lind, 1983) for details about the representation of relations between functions and equipment.

The function of the plant and its subsystems is described in terms of a very restricted set of basic flow functions. These basic functions can be interconnected into functional networks called flow structures. A flow structure is a functional network representing the plant on a level of physical detail given by the aggregation of the plant into functionally meaningful subsystems. Each physical aggregate represents a subsystem which is subject to mass or energy balance constraints. A distinction is made between internal constraints due to the system ability to e.g. store or transport mass or energy and external constraints imposed on the system by control functions in order to meet specified requirements from other systems or the environment. The representation of the internal and external constraints reflect the adaptation of process functions and control functions as achieved in process design.

Two distinct functional elements in a flow structure may correspond to two overlapping subsystems i.e., they may share components. The basis for the flow modelling is a description of the plant in terms of an abstraction hierarchy as provided by the process design and a plant flow model is obtained by mapping system aggregates (equipment, subsystems, and generic functions) into flow structures according to the principle stated above.

The following basic flow functions are used in the MFM methodology, more detailed definitions can be found in (Lind, 1983),

- storage of mass or energy,

- transport of mass or energy,

- distribution of mass or energy,

- barrier of mass or energy,

- source/sink of mass or energy,

- support function and

- control function.

The state of flow functions are characterized by performance parameters and conditions for existence of the functions can be expressed in terms of support conditions (provided by a support function). These modelling concepts are represented by symbols as shown in Figure 6 illustrating a very simple MFM model of a nuclear power plant. The example shows the application of flow modelling for the creation of multilevel models. The basis for this recursive application of the basic flow modelling concepts are due to the general nature of the conservation laws for mass and energy. In this way, we can describe a process plant from many perspectives using the same modelling concepts. As shown in this figure, we can describe a power plant as providing an energy distribution function, but we can also describe the plant on the level of pumps and valves. However, models on these two extremes of physical aggregation are related as the pumping function contributes to the overall plant function and because changes in requirements to overall plant performance (energy demand from grid) may lead to changes in the requirements on pump performance. These relations are established by proper decomposition of the flow functions in the overall plant model into lower level flow structures. This decomposition is guided by knowledge of the intentions of the plant designer. In principle any node in the flow structure can be decomposed and the flow structures generated can again be decomposed leading to a recursive application of the modelling concepts.

There are due to this recursion two interpretations of the information on any level in a multilevel model as the flow functions can be considered as specifying either goals or plant

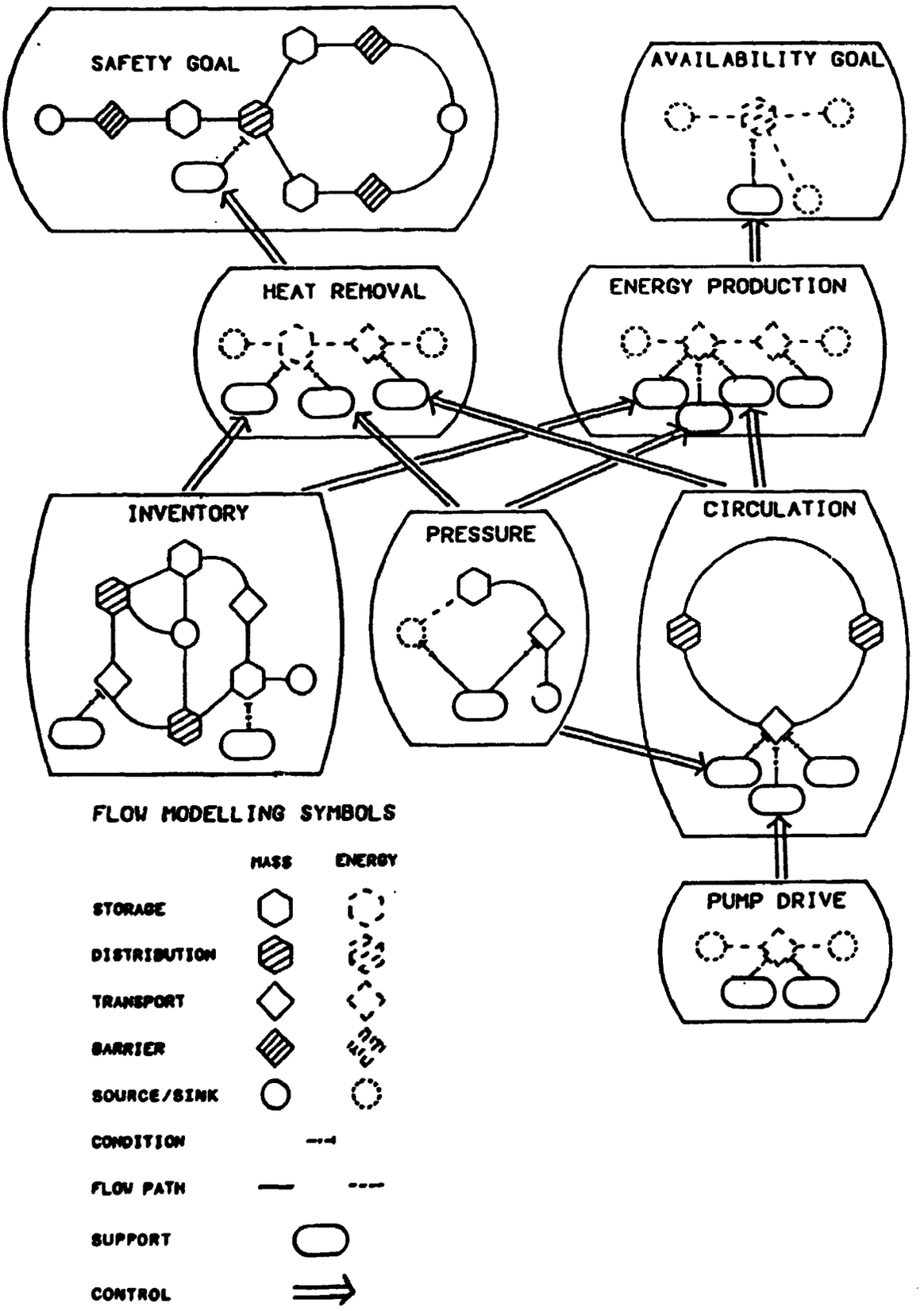


Figure 6. Multilevel flow model of a nuclear power plant of the PWR type. The model is very simplified and is only intended for illustrating the characteristics of this types of models.

functions. This is an important aspect of the MFM modelling framework. The significance of this feature can be realised by considering three consequtive levels in a MFM model. Assuming that level i describes the function of a particular plant subsystem under investigation, then level i+1 will describe why this function is required. Similarly, level i-1 will describe how the plant function on level i is established and level i will relate to what is going on the the plant subsystems considered. The triple why, what and how can be shifted upwards or downwards as the subsystem considered changes and provides a systematic functionally motivated strategy for searching through model information. The why, what and how are important for an operator in diagnosis if supported by an information display designed on the basis of an MFM plant model (Goodstein, 1982).

Generic Control Tasks

From the discussion above it appears that in the MFM framework we can define a very restricted set of socalled generic control tasks. This is basically a consequence of using MFM's for functional specification. The highly structured and recursive nature of such models leads via the interpretation of the MFM as specifying control requirements to a considerable reduction in the number of control task categories to consider. The following generic types can be identified and correspond to the control task discussed in terms of the example in Figure 3

- maintain mass and energy inventories and flows at their target values or constraints.

- change mass and energy inventories to new target values or constraints.

- reconfiguration or network switching.

Any control task can be decomposed into sequences or concurrent sets of control tasks of the generic type. The concept of

generic control tasks provide accordingly a useful tool for planning of complex control sequences. Another important property of generic control tasks is that they can be formulated within a uniform language which allows a consistent planning of control sequences which is independent of the actual physical context of the task. It could be an overall production control problem or it could be the problem in controlling lubrication oil flow to a pump (Lind, 1979 and 1983).

To each generic control function in a MFM model is associated a monitoring function. Control functions allocated to the computer, i.e., all the automated controls, should be monitored by the plant operator. The monitoring requirement can readily be defined from the MFM model, because the model specifies the control function which should be achieved, i.e., the goal of the control system and sets the standard against which actual control system performance should be evaluated.

INSTRUMENTATION SYSTEM FUNCTIONAL DESIGN

The information needed to supervise and control high level plant functions cannot be obtained directly from the plant sensors. This information should be derived by using computers for selection and processing of raw sensor data. The reliability of this computed high level information is dependent on the availability of reliable sensor signals and accordingly, it is necessary to consider the problem of signal validation. This will be discussed below, but first we will assume that validated signals are available as a basis for the computation of high level information, and consider this so-called data integration problem.

Data Integration

The solution of the data integration problem can be considered as being composed of two steps. The first step constitutes the identification of plant parameters which should be measured in order to derive a given abstract plant variable. The information to be derived is specified in the plant flow models as the performance parameters (flows and inventories of mass and energy) characterizing the individual flow functions. The actual computations to be made are derived from the physical structure of the particular system considered. A simple example illustrating the computation of the energy flow provided by the primary coolant circuit of a pressurized water nuclear power reactor is shown in Figure 7. In general there will for a given sensor configuration be many alternative ways of computing a given variable. This can be demonstrated in terms of the simple example given. If the system is performing correctly, this redundancy is not necessary, but in the case of disturbances, the redundancy is necessary in order to diagnose the disturbance.

The sensor configuration determined in this first step of the design procedure is necessary in order to support the computation of the selected performance variables. The sufficiency of the sensors to support diagnosis of postulated system faults is examined in the second step of the design procedure. This may lead to modifications and extensions of the sensor configuration identified in the first design step. The selection of variables to be measured depends in general both on economical and technical factors. The economic factors comprise the costs of alternative sensor configurations with different types and number of measuring points. The technical factors include problems of the direct measurement of certain physical variables. However, for this purpose Kalman filtering or observer techniques can be used and the approach to instrumentation design proposed here provides a systematic way of including these parameter estimation techniques into the plant information system. The approach to instrumentation system design proposed here accordingly takes advantage of available

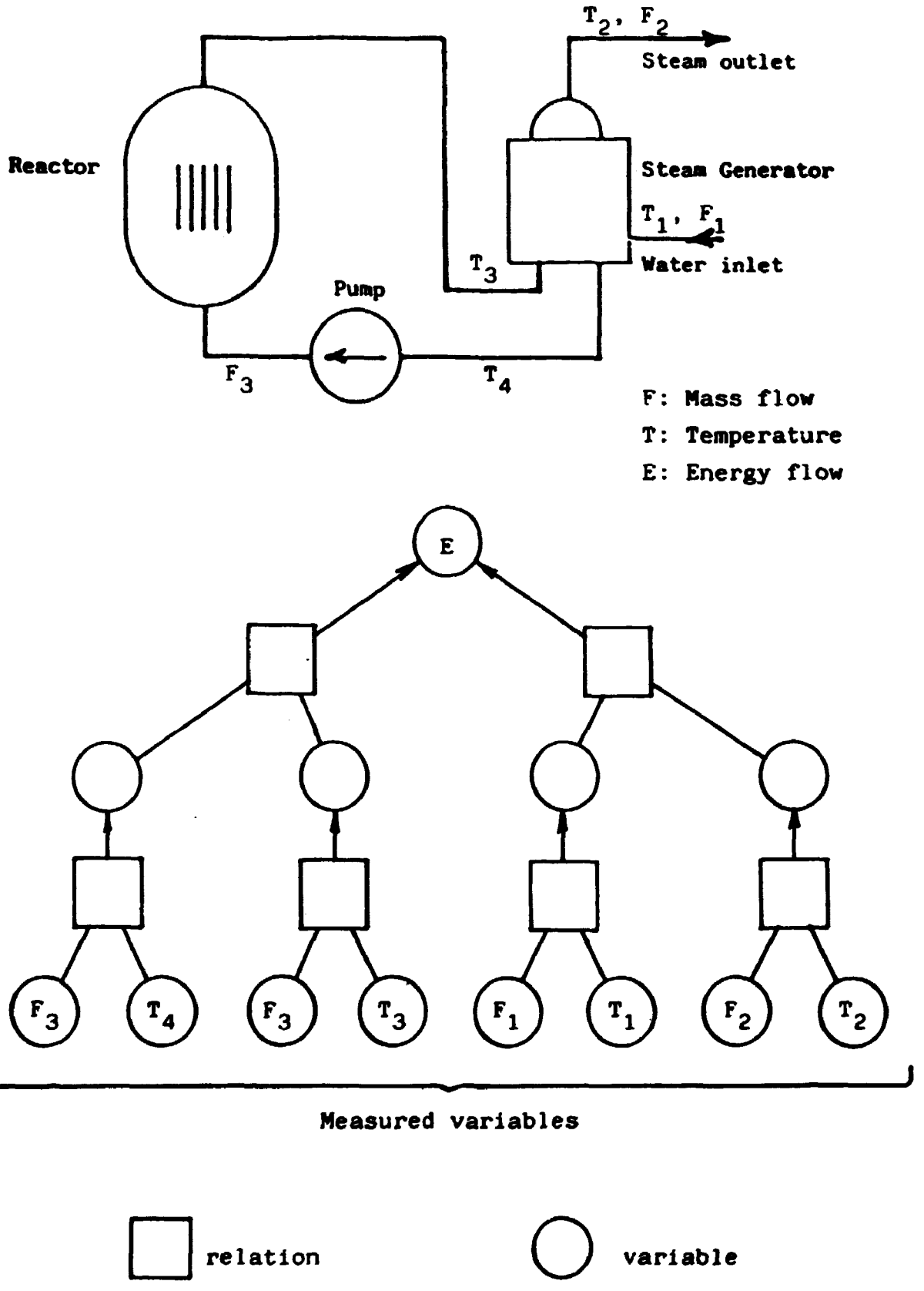
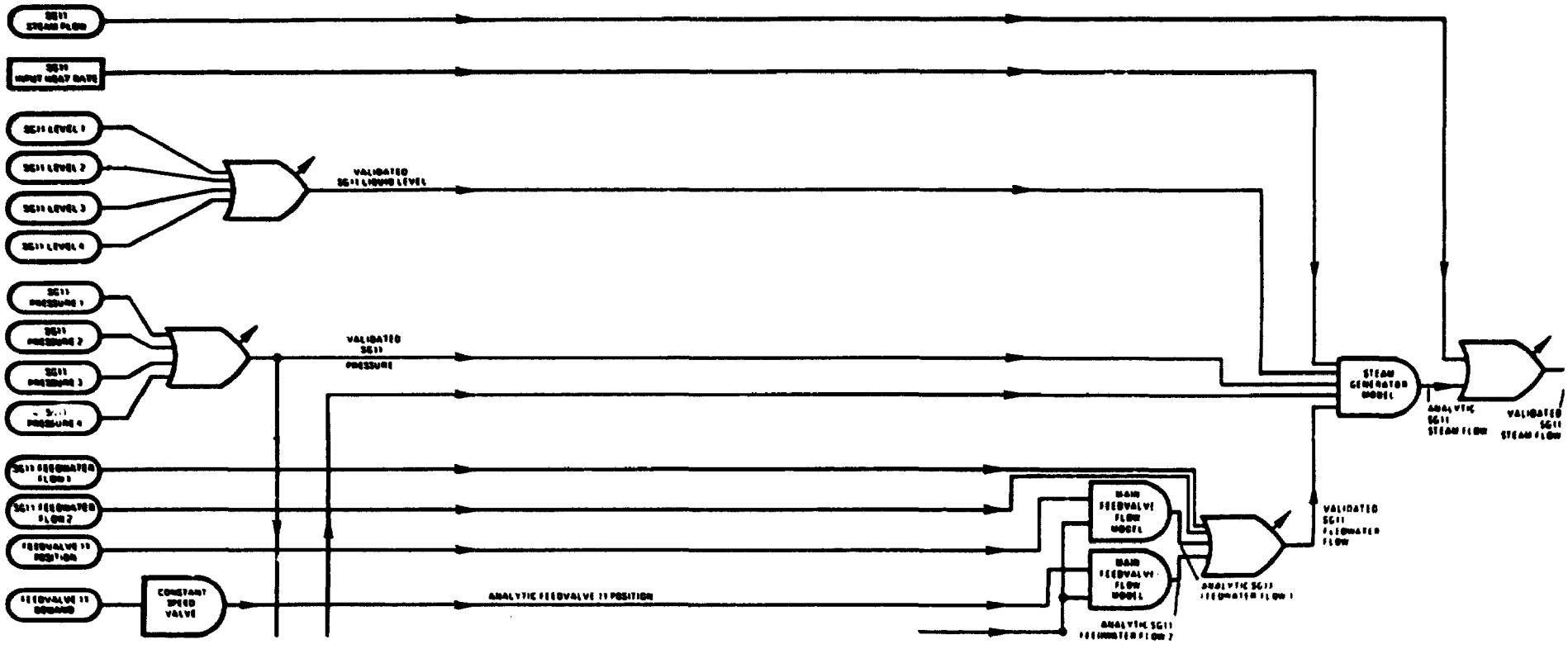
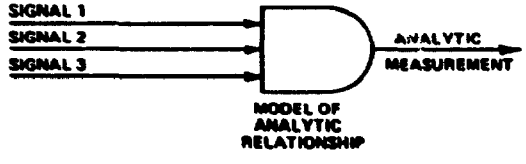
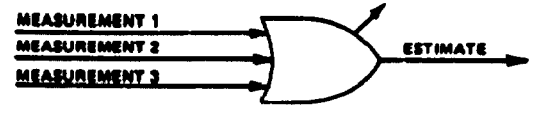


Figure 7. Simple example of data integration for a reactor coolant loop. The energy flow E transported by the loop is computed on the basis of measured flows and temperatures. Two alternative computations are possible due to redundancy.





Analytical Measurement unit



Decision/Estimator unit

Figure 8. Example of an instrumentation system for signal validation. The example is from a feedwater system in a power plant (from Meijer et. al., 1981).

distributed information processing capability, and provides a systematic approach to the design of such systems.

Sensor Validation

Reliable sensor signals are necessary for the derivation of useful high level functional information and for diagnosing disturbances. If sensor signals are not valid it is not possible to distinguish between sensor failures and process disturbances. Hardware redundancy i.e., the application of multiple sensors for the measurement of the same physical variable is usually used in order to include sensor failure detection capabilities in instrumentation systems. Recent developments in this area include also the use of so-called analytical redundancy, where synthetic measurements are derived by on-line computations using simple models of plant components. An example is included for illustration in Figure 9. The detection of sensor errors is based on the use of the so-called parity space technique (op.cit.), the figure represents only a small fraction of the structure required for validating sensor signals in the feedwater system of a nuclear power plant.

INTELLIGENT INFORMATION INTERFACES

The advantage of the approach to the design of information interfaces described here is that it relates actual plant state information with design information defining functional requirements to plant operation. However, the operation of complex production systems involves the management of a large number of production and control functions. Furthermore, operators should manage many-to-many mappings between goals and functions and between functions and equipment. Thus the use of the proposed information interface will involve an information

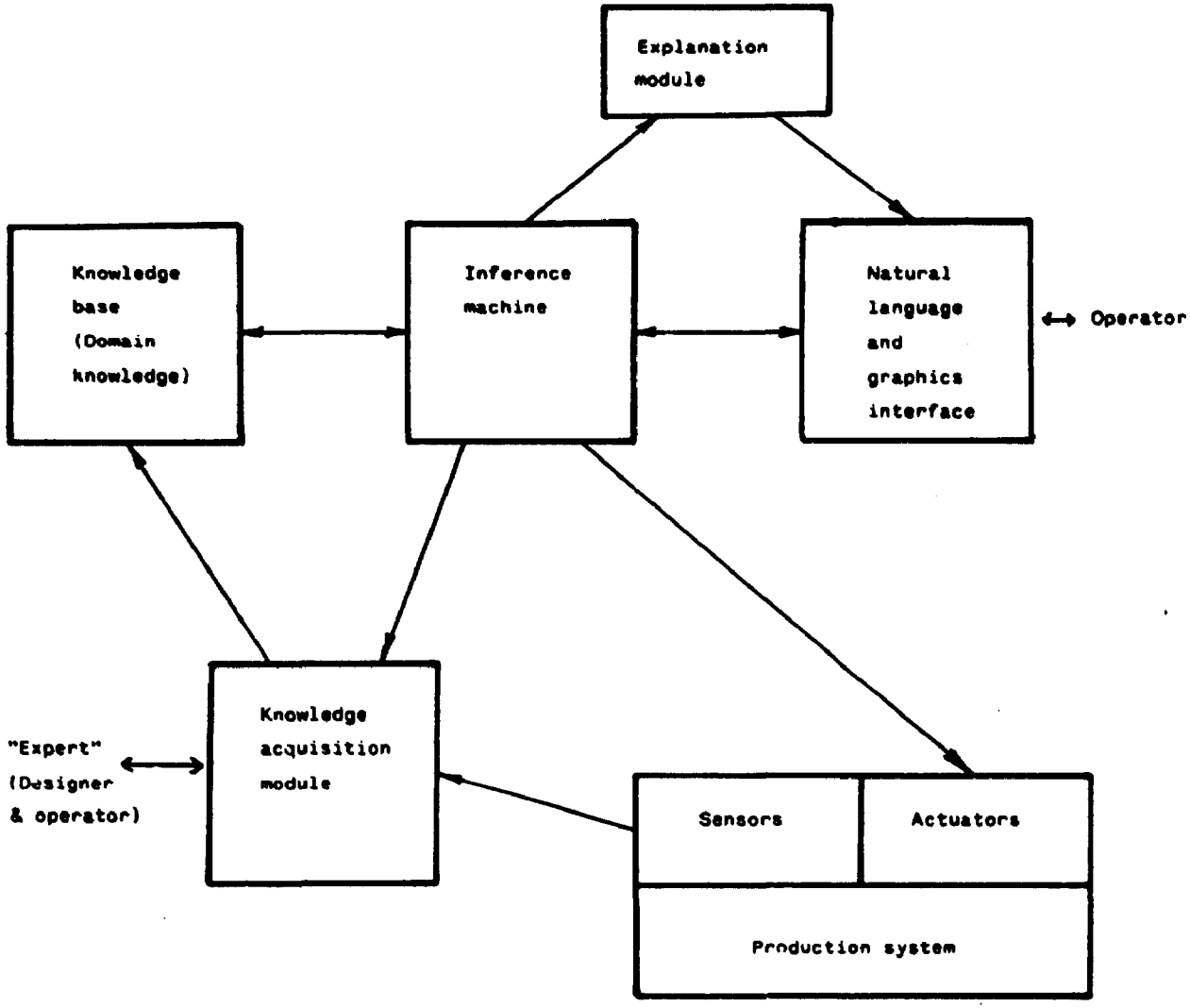


Figure 9. Basic expert systems architecture for applications in control.

retrieval problem of what particular plant functions and systems to attend to in the case of disturbance and a problem of searching through the information database. These problems can be solved by providing the operator with computer based assistance in searching through the information during diagnosis. This assistance may take several forms, it could be in the form of a question answering facility where the computer search in a database containing plant design information and actual state information to retrieve information requested by the operator. It could also be in the form of an active computer participation in the decision-making involved in diagnosis of disturbances, where the computer analyses real time plant information in order to identify operational abnormalities which may develop into serious malfunctions. The result of the analysis may then be used to advise the operator to take action or to go into a more detailed analysis of the abnormality using plant information not accessible to the computer or not amenable to consistent analysis by computer. Such a cooperative strategy for decision -making in diagnosis has been proposed (Rasmussen, 1981) in which the computer analysis is based on multilevel flow models as described earlier in the present paper. The basic philosophy is to base the computer analysis on diagnostic strategies used by plant operators and to design the interface so that it supports operators in using these strategies. This will ensure transparency of the computer analysis as it facilitates the operators' understanding of the basis for the advice generated by the computer. Due to the complexity of the deductions made by the computer the operator may require explanations of how the advice was generated, i.e., a description of the problem solving involved and a presentation of this in terms readily understandable to the operator. These facilities are considered as essential for operators' acceptance of computer advice in operations.

The software technology required for the implementation of this type of advanced information interface has been developed within Artificial Intelligence research under the name of Expert Systems or Knowledge Based Systems. This technology is

now considered mature for the development within different industrial application areas. The basic architecture of an Expert System which will be appropriate for process control applications is shown in Figure 9. The system contains five basic modules, a knowledge base, an inference mechanism, a natural language and graphics user interface, a knowledge acquisition and an explanation facility. The knowledge base will contain symbolic descriptions of the domain considered. In the actual case considered it will contain plant design information (models) to be used as a basis for diagnosis. The inference mechanism contains description of how to use the models in the knowledge base for diagnosis. This will include diagnostic strategies and general rules of logic inference. The knowledge acquisition module provides facilities for updating the knowledge base with new knowledge.

Knowledge based systems is a major research topic in the Japanese 5th generation computer project and is also considered in the European ESPRIT project. These types of information systems may be essential for the future development of reliable error tolerant production systems and provide the basis for design of user-friendly interfaces to the system operator.

REFERENCES

Eastman, C. M., "The Representation of Design Problems and Maintenance of Their Structure." IFIPS Working Conference on Application of AI and PR to CAD, Grenoble, France, March, 1978.

Goodstein, L. P., "An Integrated Display Set for Process Operators." IFAC/IFIP/IFORS/IEA Conference on Analysis, Design and Evaluation of Man-Machine Systems, Baden-Baden, F. R. Germany, September 27-29, 1982.

Lind, M., "The Use of Flow Models for Design of Plant Operating Procedures." IWG/NPPCI Specialists Meeting of procedures and systems for Assisting an Operator During Normal and Anomalous Nuclear Power Plant Operation Situations, December 5-7, 1979, Garching, F. R. Germany. Risø-M-2341.

Lind, M., "A System Modelling Framework for the Design of Integrated Process Control Systems." IASTED Conference on Applied Control and Identification ACI-83, Copenhagen, Denmark, June 28 - July 1, 1983.

Meijer, C. H. et. al., "On Line Power Plant Signal Validation Technique Utilizing Parity-Space Representation and Analytical Redundancy", EPRI NP-2110, 1981.

Mesarovic, M. D. et. al., "Theory of Hierarchical Multilevel Systems." Academic Press (1970).

Rasmussen, J., "On the Structure of Knowledge - A Morphology of Mental Models in a Man-Machine System Context." Risø-M--2192, 1979.

Rasmussen, J., "Models of Mental Strategies in Process Plant Diagnosis". In: Rasmussen, J. and Rouse, W. B. (Eds.), "Human Detection and Diagnosis of System Failures", Plenum Press, New York, 1981.

Rasmussen, J. & M. Lind, "Coping with Complexity." Risø-M-2293, 1982. European Annual Conference on Human Decision and Manual Control, Delft, 1981.

Rasmussen, J. & M. Lind, "A Model of Human Decision Making in Complex Systems and Its Use for Design of System Control Strategies." American Control Conference ACC-82, Arlington, USA, June 14-16, 1982.

Rasmussen, J.: Strategies for State Identification and Diagnosis in Supervisory Control Tasks and Design of Computer Based Support Systems. N-6-83. NKA/LIT-3.2(83)-126. To be published in "Advances in Man-Machine Systems Research. Vol. 1, W. B. Rouse (Ed.), 1983.

Rumancik, J. A., et. al., "Establishing Goals and Functions for a Plant-Wide Disturbance Analysis and Surveillance System (DASS)." IEEE Trans. Nuclear Science, NS-28, No. 1, February 1981, pp 905-912.

Simon, H. A., "The Sciences of the Artificial. The MIT Press, 2nd ed.

Sussman, G. J. & Steele Jr., G. L., "Constraints - A Language for Expressing Almost Hierarchical Descriptions." Artificial Intelligence, Vol. 14, No. 1, August 1980, pp 1-40.

Risø National Laboratory

Risø-M-2417

Risø-M-2417

Title and author(s)

INFORMATION INTERFACES FOR PROCESS PLANT DIAGNOSIS

Morten Lind

Date: February 1984

Department or group: Electronics

Group's own registration number(s): R-1-84

34 pages + tables + illustrations

Abstract

The paper describes a systematic approach to the design of information interfaces for operator support in diagnosing complex systems faults. The need of interpreting primary measured plant variables within the framework of different system representations organized into an abstraction hierarchy is identified from an analysis of the problem of diagnosing complex systems. A formalized approach to the modelling of production systems, called Multilevel Flow Modelling, is described. A MFM model specifies plant control requirements and the associated need for plant information and provide a consistent context for the interpretation of real time plant signals in diagnosis of malfunctions. The use of MFM models as a basis for functional design of the plant instrumentation system is outlined, and the use of Knowledge Based (Expert) Systems for the design of man-machine interfaces is mentioned. Such systems would allow an active user participation in diagnosis and thus provide the basis for cooperative problem solving.

Copies to

Available on request from Risø Library, Risø National Laboratory (Risø Bibliotek), Forsøgsanlæg Risø), DK-4000 Roskilde, Denmark
Telephone: (03) 37 12 12, ext. 2262. Telex: 43116

Available on request from.
Risø Library,
Risø National Laboratory, P.O. Box 49,
DK-4000 Roskilde, Denmark
Phone (02) 371212 ext. 2262

ISBN 87-550-0982-4
ISSN 0418-6435